ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

March 31, 2017

Mr. Jason Providakes
President and Chief Executive Officer
MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

Dear Mr. Providakes:

We seek your assistance in evaluating the management and performance of the Common Vulnerabilities and Exposures (CVE) program, which has become an essential service for modern cybersecurity practices. The program provides a reliable, standardized mechanism for describing information technology and cybersecurity vulnerabilities. Recent reports indicate it may not be keeping up with the increasing vulnerabilities and related risks inherent in modern cybersecurity.

Established in 1999, CVE was developed, implemented, and is currently maintained by the MITRE corporation with funding from the Department of Homeland Security. The program accepts reports of vulnerabilities in information technology products, verifies and validates the vulnerabilities, and then assigns a unique "CVE number" to each one. Once a vulnerability receives a CVE number, organizations are able to examine their systems for the vulnerability, remediate it if found, share information with partners and their customers about the impact of the flaw, and develop strategies and techniques for protecting the larger ecosystem against it and similar vulnerabilities.

Over time, CVE became the basis for additional cybersecurity services; for example, the National Institute for Standards and Technology (NIST) built additional programs on top of CVE to further strengthen and expand upon its capabilities, including the National Vulnerability Database (NVD), the Common Vulnerability Scoring System (CVSS), and the Security Content Automation Protocol (SCAP).[1] As these programs and CVE matured, organizations began to leverage them as external "add-ons" to their security efforts and integrate them directly into

---

[1] *About CVE – Widespread Adoption*, THE MITRE CORPORATION, Feb. 23, 2017, https://cve.mitre.org/about/#widespread_adoption.

cybersecurity standards, policies, and tools.[2] In short, CVE and its derivative programs have become the common language threaded through most cybersecurity products and services. CVE is critical to effective cybersecurity practices, the absence of which would severely impair the ability to address rapidly and effectively security vulnerabilities in the products and services across all sectors of American commerce.

In spring 2016, press reports revealed complaints that requests for CVE numbers for vulnerabilities reported to MITRE either were taking several weeks or months to process, or were going unanswered.[3,4] In addition, some individuals and organizations seeking CVE numbers were told that their vulnerabilities were "out of scope" for CVE, and had their vulnerabilities rejected from the program.[5]

To its credit, MITRE quickly acknowledged the problems, stating, "CVE has been experiencing an unprecedented demand for vulnerability IDs. We look forward to working with the CVE Editorial Board and the broader vulnerability management community to significantly improve stakeholder communication, and improve and scale CVE operations to reduce ID assignment response times and increase product coverage."[6] Shortly after releasing this statement, MITRE offered a series of proposed reforms.[7]

MITRE's proposal drew fierce criticism from the community, however, and it was quickly withdrawn.[8] In a second public statement addressing the community's concerns with CVE, MITRE stated, "The recent explosion of Internet-enabled devices—known as the Internet of Things—as well as the propagation of software-based functionality in systems has led to a huge increase in the number of CVE requests we have been receiving on a daily basis. We did not anticipate this rate of growth, and, as a result, were not as prepared for the latest surge in requests over the past 12 months as we had hoped. The result has been some of the delay in CVE assignments that the software security community has recently witnessed…We recognize the inconvenience that has resulted, and are working hard to come up with a solution."[9]

---

[2] *See e.g.*, NIST's Special Publication 800-53, the standard for federal government cybersecurity; the Payment Card Industry's Data Security Standard, the standard for organizations that process credit card data; the Health Insurance Portability and Accountability Act, the standard for healthcare organization cybersecurity; the Critical Infrastructure Protection Standards, the standard for electric sector cybersecurity; and the NIST Cybersecurity Framework all either directly or indirectly refer to CVE, CVSS, and NVD.

[3] Sean Sposito, *CVE, a key cybersecurity resource, is at risk inside and out*, SAN FRANCISCO CHRONICLE, Mar. 25, 2016, http://www.sfchronicle.com/business/article/CVE-a-key-cybersecurity-resource-is-at-risk-7107509.php.

[4] Catalin Cimpanu, *CVE System Sees Huge Backlog, Researchers Propose Alternative*, SOFTPEDIA, Mar. 12, 2016, http://news.softpedia.com/news/cve-system-sees-huge-backlog-researchers-propose-alternative-501665.shtml.

[5] CSO, *Over 6,000 vulnerabilities went unassigned by MITRE's CVE project in 2015*, CSO ONLINE, Sep. 22, 2016, http://www.csoonline.com/article/3122460/techology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html.

[6] *News & Events – FOCUS ON: CVE Program Status*, THE MITRE CORPORATION, Mar. 11, 2016, https://cve.mitre.org/news/archives/2016/news.html#march112016_FOCUS_ON_CVE_Program_Status.

[7] Tom Spring, *MITRE Takes on Critics Set to Revamp CVE Vulnerability Reporting*, THREATPOST, Mar. 17. 2016, https://threatpost.com/mitre-takes-on-critics-set-to-revamp-cve-vulnerability-reporting/116858/.

[8] *News & Events – FOCUS ON: CVE Program Status*, THE MITRE CORPORATION, Mar. 21, 2016, https://cve.mitre.org/news/archives/2016/news.html#march212016_FOCUS_ON_CVE_Program_Status_Update.

[9] *Id.*

Over the past year, MITRE has made several updates to the CVE program. While these changes have improved the functioning of the system, and MITRE's engagement with its stakeholder community has greatly increased, both the larger community and MITRE agree that significant work is necessary to ensure timely coverage of affected products and services.[10]

We applaud MITRE for its forthright acknowledgement of CVE's issues, and sincerely appreciate its efforts to strengthen and reform the program, and to do so in a way that actively includes its broad stakeholder community. However, it is important to recognize that these efforts are taking place against a backdrop of significant insecurity and instability within the Internet and the technologies that underpin it. The fact that CVE is struggling to meet stakeholder needs in the midst of unprecedented cyber-attacks, incidents, and compromises threatens to undermine work across the community to better secure networks and information, and risks further exacerbating other cybersecurity issues.

The explosion of connected devices and services that has been associated with the CVE program's shortcomings, while rapid, did not occur overnight. In light of this, we seek to understand how MITRE and the CVE program failed to anticipate and prepare for this growth in demand for its services and what more may be done to ensure this program can more effectively serve its essential mission.

Therefore, and pursuant to Rules X and XI of the U.S. House of Representatives, we request the following documents and information to assist the Committee in understanding the recent CVE issues and what steps MITRE is taking to ensure the program successfully adapts to current and future conditions:

1. Please provide a description and copy of all contracts associated with the CVE program, including any changes, amendments or associated modifications.

2. Please provide a timeline of the actions taken by MITRE relating to the management of fulfillment of the contract from January 01, 2011 to the present.

3. Please provide a description and copies of any analyses of the CVE program completed by or for MITRE, including, but not limited to, analyses examining the performance of the program, resource needs, and future requirements to maintain an effective and stable program, if they exist.

We appreciate your assistance with these requests and ask for your response no later than April 13, 2017. An attachment to this letter provides additional information about responding to the Committee's request. If you should have any questions, please contact John Ohly or Jessica Wilkerson of the Committee staff at (202) 225-2927.
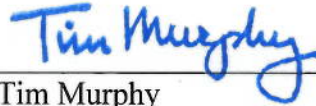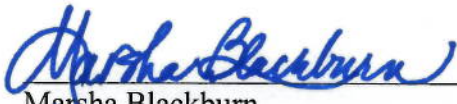
Sincerely,

---

[10] *See* "Minutes from CVE Editorial Board Teleconference Meeting[s]" *and* "FOCUS ON: CVE Program Status Updates" *at* https://cve.mitre.org/news/archives/2016/news.html.

Greg Walden
Chairman
Committee on Energy and Commerce

Tim Murphy
Chairman
Subcommittee on Oversight and
   Investigations

Marsha Blackburn
Chairman
Subcommittee on Communications and
   Technology

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
   and Consumer Protection

cc: The Honorable Frank Pallone, Jr., Ranking Member
        Committee on Energy and Commerce

        The Honorable Diana DeGette, Ranking Member
        Subcommittee on Oversight and Investigations

        The Honorable Michael F. Doyle, Ranking Member
        Subcommittee on Communications and Technology

        The Honorable Janice Schakowsky, Ranking Member
        Subcommittee on Digital Commerce and Consumer Protection

Attachment